IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A wireless communication system including a plurality of terminals, comprising:

an ad-hoc network;

a first terminal configured to send, using the ad-hoc network, a signal that includes beacon information having a first identifier that identifies the origin of the sent beacon and a second ~~an~~ identifier that identifies [[a]] an issuing terminal of a ~~type of~~ certificate of privilege; and

a second terminal configured to send, using the ad-hoc network, an authentication request to the first terminal in response to the signal sent from the first terminal by providing the ~~type of~~ certificate of privilege which matches the second identifier,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 2 (Previously Presented): A wireless communication system including a plurality of terminals, comprising:

an ad-hoc network;

a first terminal configured to send, using the ad-hoc network, a signal that includes beacon information indicating an operation mode of the first terminal; and

a second terminal configured to send, using the ad-hoc network, an authentication request to the first terminal in response to the signal sent from the first terminal when the operation mode of the first terminal coincides with an operation mode of the second terminal, by providing a certificate of privilege indicating a right concerning the operation mode of the second terminal,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 3 (Currently Amended): A terminal comprising:

a certificate of privilege table for storing a certificate of privilege indicating an access right of the terminal;

receiving means for receiving a signal sent from a different terminal including beacon information having a first identifier that identifies the origin of the sent beacon and a second ~~an~~ identifier that identifies [[a]] an issuing terminal of a ~~type of~~ certificate of privilege from the different terminal; and

authentication request means for sending an authentication request to the different terminal by providing the certificate of privilege stored in the certificate of privilege table that matches the second identifier contained in the signal received by the receiving means,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 4 (Original): A terminal according to claim 3, wherein the identifier is a terminal identifier of a terminal that has issued the certificate of privilege.

Claim 5 (Previously Presented): A terminal according to claim 3, further comprising:

a certificate-of-privilege issuing terminal list table for storing a public key certificate of a terminal that has issued the certificate of privilege;

authentication-request receiving means for receiving a second authentication request from the different terminal in response to the authentication request sent from the authentication request means; and

verification means for verifying a second certificate of privilege contained in the second authentication request received by the authentication-request receiving means by using a public key contained in the public key certificate stored in the certificate-of-privilege issuing terminal list table.

Claim 6 (Original): A terminal according to claim 5, wherein:

the identifier is a terminal identifier of a terminal that has issued the certificate of privilege; and

the certificate-of privilege issuing terminal list table stores the terminal identifier of the terminal that has issued the certificate of privilege, the public key certificate of the terminal that has issued the certificate of privilege, and a storage location of the certificate of privilege in the certificate of privilege table in association with each other.

Claim 7 (Currently Amended): A terminal comprising:

a certificate of privilege table for storing a certificate of privilege indicating an access right of the terminal; and

sending means for sending a different terminal a signal including beacon information having a first identifier that identifies the origin of the sent beacon and a second ~~an~~ identifier that identifies [[a]] an issuing terminal of a ~~type of~~ certificate of privilege stored in the certificate of privilege table,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 8 (Original): A terminal according to claim 7, wherein the identifier is a terminal identifier of a terminal that has issued the certificate of privilege.

Claim 9 (Currently Amended): A terminal comprising:

a certificate of privilege table for storing a plurality of certificates of privilege indicating an access right of the terminal;

selection means for providing an instruction to select one of the plurality of certificates of privilege stored in the certificate of privilege table; and

sending means for sending a different terminal a signal including beacon information having a first identifier that identifies the origin of the sent beacon and a second ~~an~~ identifier that identifies [[a]] an issuing terminal of a ~~type of~~ the certificate of privilege selected by the selection means,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 10 (Original): A terminal according to claim 9, wherein the identifier is a terminal identifier of a terminal that has issued the certificate of privilege.

Claim 11 (Previously Presented): A terminal comprising:

a certificate of privilege table for storing a certificate of privilege indicating an access right of the terminal;

a status table for storing an operation mode of the terminal;

receiving means for receiving a signal including beacon information having an operation mode of a first terminal from the different terminal; and

authentication request means for sending, when the operation mode of the terminal and the operation mode of the different terminal coincide with each other, an authentication

request to the different terminal by providing the certificate of privilege stored in the certificate of privilege table,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 12 (Previously Presented): A terminal according to claim 11, further comprising:

a certificate-of-privilege issuing terminal list table for storing a public key certificate of a terminal that has issued the certificate of privilege;

authentication-request receiving means for receiving a second authentication request from the first different terminal in response to the authentication request sent from the authentication request means;

verification means for verifying a second certificate of privilege contained in the second authentication request received by the authentication-request receiving means by using a public key contained in the public key certificate stored in the certificate-of-privilege issuing terminal list table; and

operation-mode checking means for determining, after the second certificate of privilege is successfully verified by the verification means, that the second authentication request is rejected when the operation mode of the different terminal is not permitted by an operable mode contained in the second certificate of privilege.

Claim 13 (Original): A terminal according to claim 12, wherein:

the identifier is a terminal identifier of the terminal that has issued the certificate of privilege; and

the certificate-of-privilege issuing terminal list table stores the terminal identifier of the terminal that has issued the certificate of privilege, the public key certificate of the terminal that has issued the certificate of privilege, and a storage location of the certificate of privilege in the certificate of privilege table in association with each other.

Claim 14 (Previously Presented): A terminal according to claim 12, further comprising:

a policy table for storing a management policy to be used with the different terminal; and

management-policy setting means for setting a management policy contained in the second certificate of privilege in the policy table when the operation-mode checking means determines that the second authentication request is not rejected.

Claim 15 (Previously Presented): A terminal comprising:

a status table for storing an operation mode of the terminal; and

sending means for sending a signal including beacon information having the operation mode of the terminal to a different terminal.

Claim 16 (Currently Amended): A terminal comprising:

a certificate of privilege table for storing a certificate of privilege indicating an access right of the terminal;

a status table for storing an operation mode of the terminal;

receiving means for receiving from a different terminal a signal including beacon information having a first identifier that identifies the origin of the sent beacon and a second

~~an~~ identifier that identifies [[a]] an issuing terminal of a ~~type of~~ certificate of privilege and an operation mode of the different terminal; and

authentication request means for sending, when the operation mode of the terminal and the operation mode of the different terminal coincides with each other, an authentication request to the different terminal by providing the certificate of privilege that matches the second identifier contained in the signal received by the receiving means,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 17 (Original): A terminal according to claim 16, wherein the identifier is a terminal identifier of a terminal that has issued the certificate of privilege.

Claim 18 (Previously Presented): A terminal according to claim 16, further comprising:

a certificate-of-privilege issuing terminal list table for storing a public key certificate of a terminal that has issued the certificate of privilege;

authentication-request receiving means for receiving a second authentication request from the different terminal in response to the authentication request sent from the authentication request means;

verification means for verifying a second certificate of privilege contained in the second authentication request received by the authentication-request receiving means by using a public key contained in the public key certificate stored in the certificate-of-privilege issuing terminal list table; and

operation-mode checking means for determining, after the second certificate of privilege is successfully verified by the verification means, that the second authentication

request is rejected when the operation mode of the different terminal is not permitted by an operable mode contained in the second certificate of privilege.

Claim 19 (Original): A terminal according to claim 18, wherein:

the identifier is a terminal identifier of the terminal that has issued the certificate of privilege; and

the certificate of privilege issuing terminal list table stores the terminal identifier of the terminal that has issued the certificate of privilege, the public key certificate of the terminal that has issued the certificate of privilege, and a storage location of the certificate of privilege in the certificate of privilege table in association with each other.

Claim 20 (Previously Presented): A terminal according to claim 18, further comprising:

a policy table for storing a management policy to be used with the different terminal; and

management-policy setting means for setting a management policy contained in the second certificate of privilege in the policy table when the operation mode checking means determines that the second authentication request is not rejected.

Claim 21 (Previously Presented): A terminal comprising:

a certificate of privilege table for storing a certificate of privilege indicating an access right of the terminal;

a status table for storing an operation mode of the terminal; and

sending means for sending a different terminal a signal including beacon information having an identifier that identifies the type of certificate of privilege of the certificate of privilege table and the operation mode of the terminal,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 22 (Original): A terminal according to claim 21, wherein the identifier is a terminal identifier of a terminal that has issued the certificate of privilege.

Claim 23 (Currently Amended): A terminal comprising:

a certificate of privilege table for storing a plurality of certificates of privilege indicating an access right of the terminal;

a status table for storing an operation mode of the terminal;

selection means for providing an instruction to select one of the plurality of certificates of privilege stored in the certificate of privilege table; and

sending means for sending a different terminal a signal including beacon information having a first identifier that identifies the origin of the sent beacon and a second ~~an~~ identifier that identifies [[a]] an issuing terminal of a ~~type of~~ the certificate of privilege selected by the selection means and the operation mode of the terminal,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 24 (Original): A terminal according to claim 23, wherein the identifier is a terminal identifier of a terminal that has issued the certificate of privilege.

Claim 25 (Currently Amended): A processing method for use in a terminal which includes a certificate of privilege table for storing a certificate of privilege indicating an access right of the terminal, and a status table for storing an operation mode of the terminal, said processing method comprising:

a step of receiving from a different terminal a signal including beacon information having a first identifier that identifies the origin of the sent beacon and a second ~~an~~ identifier that identifies [[a]] an issuing terminal of a ~~type of~~ certificate of privilege and an operation mode of the different terminal; and

a step of sending, when the operation mode of the terminal and the operation mode of the different terminal coincides with each other, an authentication request to the different terminal by providing the certificate of privilege stored in the certificate of privilege table that matches the second identifier contained in the signal,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.

Claim 26 (Previously Presented): A processing method for use in a terminal which includes a certificate of privilege table for storing a plurality of certificates of privilege indicating an access right of the terminal, and a status table for storing an operation mode of the terminal, said processing method comprising:

a step of providing an instruction to select one of the plurality of certificates of privilege stored in the certificate of privilege table; and

a step of sending a signal a different terminal including beacon information having an identifier that identifies a type of the selected certificate of privilege and the operation mode of the terminal,

wherein the certificate of privilege includes encrypted data for certifying the second terminal.